UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,822	03/26/2004	Blayn W. Beenau	60655.8300	2821

20322 7590 04/07/2006

SNELL & WILMER
ONE ARIZONA CENTER
400 EAST VAN BUREN
PHOENIX, AZ 850040001

EXAMINER	
WALSH, DANIEL I	
ART UNIT	**PAPER NUMBER**
2876	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/708,822	BEENAU ET AL.	
	Examiner	Art Unit	
	Daniel I. Walsh	2876	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Receipt is acknowledged of the RCE received on 24 January 2006.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 19 and 23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The Examiner notes that claim 19 recites that the secondary security procedure includes sending a signal to the host to notify that at least one of the preset transaction limitation and an established rule for the transponder is being violated. The Examiner does not find support for this in the specification or the originally filed claims.

The Examiner notes that claim 23 recites first and second user information, primarily and secondarily associated with a biometric sample, as per claim 14, upon which claim 23 depends. However, the specification teaches that the sample is of one user (paragraph [0158] which teaches that a fob user can have a debit card account secondarily associated with his right index fingerprint so that if primary account is overdrawn or unavailable, the secondary account will be

accessed to complete the transaction). The specification does not teach that the samples involved in the primary and secondary association are from different users.

Appropriate correction is required.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 23 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is vague/indefinite how "a sample" can include information corresponding to different users.

Appropriate clarification/correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor

and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 1-13, and 17-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black (US 6,925,565) in view of Huennekens et al. (US 2003/0004866).

Re claims 1 and 22, Black teaches a transponder reader system configured with a biometric security device (fingerprint sensor FIG. 1A), the system comprising a transponder (FIG. 1A) configured to communicate with a reader (transponder FIG. 1A), where the reader and biometric security device communicate with a host (host computer FIG. 1A+), the biometric security device comprising a biometric sensor (fingerprint sensor FIG. 1A) configured to detect a proffered biometric sample, the biometric sensor configured to communicate with the system. Though silent to a verification device to verify the sample (authenticity), the Examiner notes that it is well known and conventional in the art to verify that biometric samples are real (living finger, actual eye, etc.) by using procedures such as measuring temperature, blood flow, etc. Accordingly, the Examiner notes that it would have been obvious to one of ordinary skill in the art to use a well-known verification device (with the sensor, for example) to verify the authenticity of the sample, for security purposes, as means to facilitate a secure payment transaction.

Black is silent to the verification device configured to verify whether the biometric sample is associated with a preset transaction limitation and whether the payment transaction is in compliance with the preset transaction limitation.

The Examiner notes that it is well known and conventional in the art for credit cards, for example, to have an associated credit limit, which can be interpreted as a maximum transaction amount. Specifically, Huennekens et al. teaches a credit limit is associated with a credit card account, and that during a purchase, the credit limit is verified (paragraph [0005]+).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Huennekens et al.

One would have been motivated to do this for security, for example, to have a credit limit on the purchasing power. The Examiner notes that the verification device (interpreted as the device facilitating the financial transaction) checks the credit limit of the card for the purchase. As it has been discussed above that the biometric is required to authenticate the user for the card/transaction, and card/transaction has a preset transaction limitation, the Examiner has interpreted that the biometric is associated with the preset transaction limitation in order to verify and complete the financial transaction.

Re claim 2, Black teaches the biometric sensor communicates with the transponder reader transaction system via one of a transponder, reader, and a network (FIG. 1A), which shows the interconnection of the biometric sensor with the system. Though silent to a network communication, the Examiner notes that as the system is used for purchases in a commercial environment (stores), it would have been obvious to have a network connection in order for data to be shared between terminals/registers in order to reduce costs and maintain a central data storage for ease of updating information, record keeping, etc., as an obvious expedient well within the skill in the art.

Re claim 3, it is understood that the biometric sensor is configured to facilitate a finite number of scans (one for example) in order to receive a sample.

Re claim 4, Black teaches that access is only granted (to finish a transaction) when the stored and proffered data corresponds (col 6, lines 15+). This is interpreted as employing a security procedure when the proffered sample differs from the log/stored data, because access is denied, in a manner that is conventional in the art when authorization fails. Additionally, The Examiner notes that the use of security features when attempting access is well known and conventional in the art for security purposes (the use of secondary procedures, locking users out of a system when attempts failed, PINs, encryption, etc.). As Black teaches that the customer registers using a fingerprint (abstract) it would have been obvious to one of ordinary skill in the art to register the fingerprint at a sensor (in order to receive the print). As the fingerprint is subsequently stored as the reference print, the Examiner has interpreted this to include the sensor being configured to store log data comprising one of a detected biometric sample, a processed biometric sample, and a stored biometric sample, as it makes sense for the sensor receiving the sample to receive it to store in a record. Additionally, as the sensor receives the biometric sample the Examiner notes that the data is necessarily temporarily stored in the sensor (memory associated with the sensor), as its received, such as in a buffer, as is conventional in the art. The Examiner has interpreted that the sensor is configured to store the data in a memory, as the claims do not recite that the sensor stores the data in the sensor itself. Additionally, the Examiner notes the addition of limitations stating that storage occurs in a memory integrated with the sensor/separate from the sensor do not appear to be patentably distinct over the teachings of the prior art, as the sensor is used to receive data that is stored (somewhere). The

data is eventually communicated into a record format, so it does not appear critical where the log data is first stored, but namely where it ends up (record).

Re claim 5, Black teaches (col 6, lines 56+) that the customer record can be stored locally or remotely. The Examiner notes that though Black is silent to a data packet being stored in a database, Black teaches that the customer record can included one of a proffered biometric sample, registered biometric sample, proffered and registered user information, terrorist information, and criminal information (FIG. 5A+). The Examiner notes that it would have been obvious to one of ordinary skill in the art to store such information in a database format, as is conventional in the art, for organization of data and ease/quickness of retrieval.

Re claim 6, as discussed above, Black teaches that the data is stored remotely or locally. Accordingly, the Examiner notes that if stored locally or if stored remotely, it would have been obvious to one of ordinary skill in the art to store it on one of the transponder (as discussed above), a remote server/merchant server/transponder reader system, for example. One would have been motivated to store it locally so that all the data is on the transponder itself, so transactions can be completed with minimal additional/outside effort. One would have been motivated to store it remotely/on a server for security purposes. Additionally, the Examiner notes that whether stored remotely or locally, it is still part of the transponder reader system. Though silent to a server, the Examiner notes that servers are well-known and conventional means for storing data that is accessed remotely/over a network, or servers as a shared resource. One would have been motivated to use a server in order to store and communicate the information over a network.

Re claim 7, as it been discussed above as to storing record and being accessed to authenticate samples/users, it would have been obvious to have it operated by an authorized sample receiver in order to have increased security and reliability.

Re claim 8, it has been discussed above that a proffered sample is compared with a stored sample for authentication/verification. Though silent to a comparison device, the Examiner note that it would have been obvious to use a comparison device to efficiently and reliably perform the comparisons (such as a processor, controller, etc.) as is known in the art.

Re claim 9, Black teaches that a comparison is made between a proffered and stored biometric sample (fingerprint sensor), and therefore compares prints. Additionally, the Examiner notes that though the teachings of Black are silent to other of the biometric characteristics, the Examiner notes that such characteristics are well known and conventional in the art for authenticating a sample (biometric). Selection of a particular biometric characteristic is therefore an obvious expedient to verify a sample based on different authenticating characteristics.

Re claim 10, it has been discussed above that a comparison is performed. The Examiner notes that it would have been obvious to one of ordinary skill in the art for a processor/microprocessor/controller (interpreted as a protocol/sequence controller) to perform the comparison, in order to have an electronic means to reliably and quickly performing the comparison, in a manner that is conventional in the art.

Re claim 11, the Examiner notes that as a sample is stored, it is interpreted as registered.

Re claim 12, Black teaches that a customer's account is linked to the biometric data, and can be used for payment (abstract). This is interpreted to include the sample being associated with at least one of personal information, credit card information, debit card information, savings

account information, and loyalty point information, as such information would be associated in order to conduct payment. Additionally, the Examiner notes that though Black does not teach all of the different types of information (as the claims do not recite that all of the listed information is required), such information would be obvious to include in order to link a person and information for record keeping purposes, as is conventional in the art.

Re claim 13, it has been discussed above how a register biometric sample for a user is stored and compared against a proffered sample to complete a transaction. Though Black is silent to different biometric samples, the Examiner notes that it is obvious that the system can include different samples in order to accommodate different users of the system, as for example, different users have different fingerprints (fingerprints are unique for each person). Accordingly, it would have been obvious for biometric samples to be associated with a different credit card information, debit card information, etc. as per the uniqueness of each customer. The claims do not recite that the different samples are required to be associated with the same person. Therefore, as Black is drawn towards commercial transactions, it is obvious that multiple people would be involved (different customers) and accordingly there would be different samples due to different customers.

Re claim 17, Black teaches that a light can advise the customer that the payment has been accepted. Though Black is silent to teaching notification is provided, the Examiner notes that it is well known and conventional in the art when conducting a financial transaction such as a credit card purchase, for notification to be provided to the primary account holder that the primary account is being accessed, such as through a message displaying or playing "Thank You" or just through mere completion of the transaction/parts of the transaction without error

messages. Therefore, it would have been obvious to notify the user via such conventional methods such as on screen displays, audible/visual cues, etc. that the transaction is proceeding/the account is being access/used, in order to provide notification that the transaction completed. Additionally, the Examiner notes that it has been discussed above that failure of authentication results in failure of a transaction. Therefore, positive notification is merely an equivalent that is well within the skill in the art to keep the user notified of the status of the transaction.

Re claim 18, Black teaches the verification device is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction (abstract).

Re claim 19, the teachings of Black have been discussed above. Though Black is silent to sending a signal to the hose to notify that a rule is violated, the Examiner notes that it is understood that if access is blocked due to lack of proper authentication, that the host would be well aware of this because the host is the entity through which authentication occurs. Additionally, it would have been obvious to keep track of failed/illegal attempts on an account/transaction for record keeping purposes relating to security, such as with other financial transactions. Illegally attempting or failure to be verified is interpreted as a rule of the transponder being violated.

Re claim 20, as discussed above, credit cards are well known to have transaction limitations (credit limits) which can be interpreted as a maximum transaction amount. Additionally, the Examiner notes that other limitations that are well known and conventional in the art include maximum amount of transactions in a time period, maximum amount of money

per transaction. Such variations are obvious expedients, for different levels of security, for example.

Re claim 21, Black teaches (FIG. 1A) that the host computer can store the reference data. The Examiner has interpreted the host computer as biometric information register with at least one of a third party biometric security vendor and a government agency. The Examiner notes that as the transactions can take place remotely, it is obvious that the host computer can be such a party as claimed (for example the card/fob company the user is registered with) as a means for securely providing the biometric information to facilitate a transaction at a point of sale terminal, for example.

5. Claim 13 is alternatively rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Huennekens et al. in view of Martizen et al, as cited in the previous action.

The teachings of Black/Huennekens et al. have been discussed above.

Black/Huennekens et al. is silent to different samples (of one person) associated with different one of personal information, credit card information, etc.

Re claim 13, Martizen et al. teaches different registered biometric samples are associated with a different one of personal information, credit card information, debit card information, savings account information, and loyalty point information (FIG. 6A).

At the time the invention was made it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Martizen et al.

One would have been motivated to do this in order to permit multiple accounts to be securely associated with different samples, for different levels/requirements for access.

6. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Huennekens et al./Martizen et al., as discussed above, in view of Moebs et al., as cited in the previous Office Action.

The teachings of Black/ Huennekens et al./Martizen et al. have been discussed above. Martizen et al. teaches a biometric samples is associated with at least one of a first user account, wherein the first account comprises personal information, credit card information, debit card information, savings account information, and loyalty point information, and wherein the information, where the first account is different than the second account (FIG. 6A), but is silent to primary and secondary associating.

Moebs et al. teaches that a customer can avoid overdraft by preauthorizing the financial institution to tie the customer's checking account to one or more of the customers other accounts (paragraph [0017]). The Examiner notes that such protection is well known in the art, and it would be obvious that by linking the overdraft account to the primary account, that a primary and secondary association is established. Additionally, it would have been obvious for the accounts to have account information, personal information, as is conventional with accounts in order to identify and keep track of them.

At the time the invention was made it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/ Huennekens et al./Martizen et al. with those of Moebs et al.

One would have been motivated to do this to provide for overdraft protection, for example. The Examiner notes that by being associated with different accounts, the Examiner has interpreted such association to include information, as is conventional in the art, where accounts

have information associated with them for record keeping purposes, for example. By being associated with an account, the Examiner has interpreted that the sample is associated with the account information.

7. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Huennekens et al., as discussed above, in view of Teicher, as cited in the previous Office Action.

The teachings of Black/Huennekens et al. have been discussed above.

Black/Huennekens et al. is silent to mutual authentication upon verification of the proffered biometric sample.

The Examiner notes that mutual authentication is well known and conventional in the art, for security purposes, to ensure that a valid reader and device are communicating. It would have been obvious to one of ordinary skill in the art to mutually authenticate upon verification of the biometric sample, in order to ensure that the transponder and reader are authentic and should be communicating with each other. Specifically, Teicher teaches a contactless smart card that begins mutual authentication after an input (PIN) is entered (col 7, lines 35+).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Teicher.

One would have been motivated to do this to employ well-known contactless security measures between the reading device and remote device to enhance security after an input is verified.

8. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Huennekens et al., as discussed above, in view of Goodman et al. as cited in the previous Office Action.

The teachings of Black/Huennekens et al. have been discussed above. Black teaches that the transaction is blocked when the biometrics do not match, as is conventional in the art, but Black is silent to deactivating the transponder upon rejection of the biometric sample that is proffered.

The Examiner notes that it is well known and conventional in the art, for cards to be disabled, as a security measure, if a predetermined amount of attempts to enter a password/code/identifier are detected. Specifically, Goodman et al. teaches deactivation of a card if a predetermined amount of incorrect PIN attempts are detected (paragraph [0029]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Huennekens et al. with those of Goodman et al.

One would have been motivated to do this in order to increase the security of the system by disabling the card after incorrect inputs.

Though Goodman et al. is silent to using a biometric input, the Examiner notes that Goodman et al. is relied upon for teaching the disabling of access when a matching input is not received. As it is conventional to not authorize a transaction if an input does not match stored information, it would have been obvious to expand upon such teachings to include those of Goodman et al. to include disabling so that unauthorized use cannot occur, and to put a limit on the amount of attempts to reduce the chance of illegal attempts, especially as Black replaces PIN input with biometric inputs.

9. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Huennekens et al., as discussed above, in view of Haala, as cited in the previous Office Action.

The teachings of Black/Huennekens et al. have been discussed above.

Black/Huennekens et al. is silent to a secondary security procedure and sending a signal to the host to notify that a rule for the transponder is being violated.

It has been discussed above, and in the previous Office Action that the use of a secondary security procedure is well known and conventional for security. Additionally, it is well known in the art that when authentication is not performed (user not verified) that a transaction will not be completed. With regards to sending a signal to the host to notify that a rule is being violated, it would have been obvious to do so because if the transaction is blocked due to improper authentication (failed authentication), it would be obvious for the host to be aware of the situation, since the host is the entity through which authentication is recorded/takes place, and records would be stored.

Specifically, Haala teaches secondary security procedures (providing user information) (FIG. 3).

At the time the invention was made, it would have been obvious to combine the teachings of Black/Huennekens et al. with those of Haala.

One would have been motivated to do this in order to have increased security. The Examiner has interpreted that by not being authorized (failing), a rule for the transponder is being violated (i.e. fraudulent access is attempted, for example).

10. Claim 19 is alternatively rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Huennekens et al., as cited above, in view of Black (US 2005/0122209).

The teachings of Black/Huennekens et al. have been discussed above. Though Black is silent to sending a signal to the host to notify a rule is being violated, the Examiner notes that it has been discussed above that a transaction only completes when data is verified. Accordingly, it would have been obvious to send records to the host when failed attempts are made, in order to keep detailed records for monitoring activity (possible theft, etc) of the system.

Black/Huennekens et al is silent to a secondary security procedure.

Black '209 teaches secondary security procedures through comparing the electronic signature (abstract). Black teaches record storing through the use of a transaction record (paragraph [0125]). Though silent to forwarding the information to a host, it would have been obvious for the information to be forwarded/stored at the host for security and central accessibility.

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Huennekens et al. with those of Black '209.

One would have been motivated to do this for increased security.

The Examiner has interpreted that by not being authorized (failing), a rule for the transponder is being violated (i.e. fraudulent access is attempted, for example).

Additional Remarks

11. The Examiner notes that art rejections of claim 19 have been repeated above even though the claims are subject to 112 rejections as well, because the art rejections had already been previously made.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel I. Walsh whose telephone number is (571) 272-2409. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel I Walsh
Examiner
Art Unit 2876
3-20-06